MacEwan University

Exploring Social Media Sharing

The Nature of Private Information Shared by *Instagram* Users

Melanie Modrall

Abstract

This research explores the nature of social media sharing of personally identifiable information on *Instagram* by conducting a content analysis on a total of ten profiles and five posts per profile, selected randomly. Data was categorized by three methods of information sharing: profile, captions, and posts containing images or videos. Fourteen themes were discovered for sharing in profiles and captions, while fifteen were found for images and videos. Results showed users were most likely to share information in their profile (64.1%) and most commonly shared their gender presentation, face, and location. This supports previous research concerning privacy and security risks from social media sharing, indicating that these concepts need to be re-evaluated in order to maintain cyber security.

Introduction

Social media is everywhere, with access readily available on cellphones, computers, tablets, and other electronic devices. When people share aspects of their lives with others online, they do not always consider who has access to this information and how it is being used (Hogan, 2010). Privacy and security settings exist, however, this does not ensure protection from the risks involved by revealing aspects of our personal lives to known and unknown online audiences (O'Neil, 2001). There is little research addressing the links between privacy concerns, the nature of personal information shared on social media sites, and the actions taken to ensure account security (O'Neil, 2001).

The purpose of this content analysis was to analyze profiles and uploaded visual content depicting personal information on *Instagram*, with various criteria considered in exploring the nature and frequency in which information is presented. The ways in which users can share information on this platform include user profiles, captions, and posts containing images or videos (Instagram, 2018). Exploring what people are comfortable sharing on social media sites provides insight into what is considered "private." This is especially helpful in improving future services, where private information is used in maintaining online security and preventing identity theft.

Method

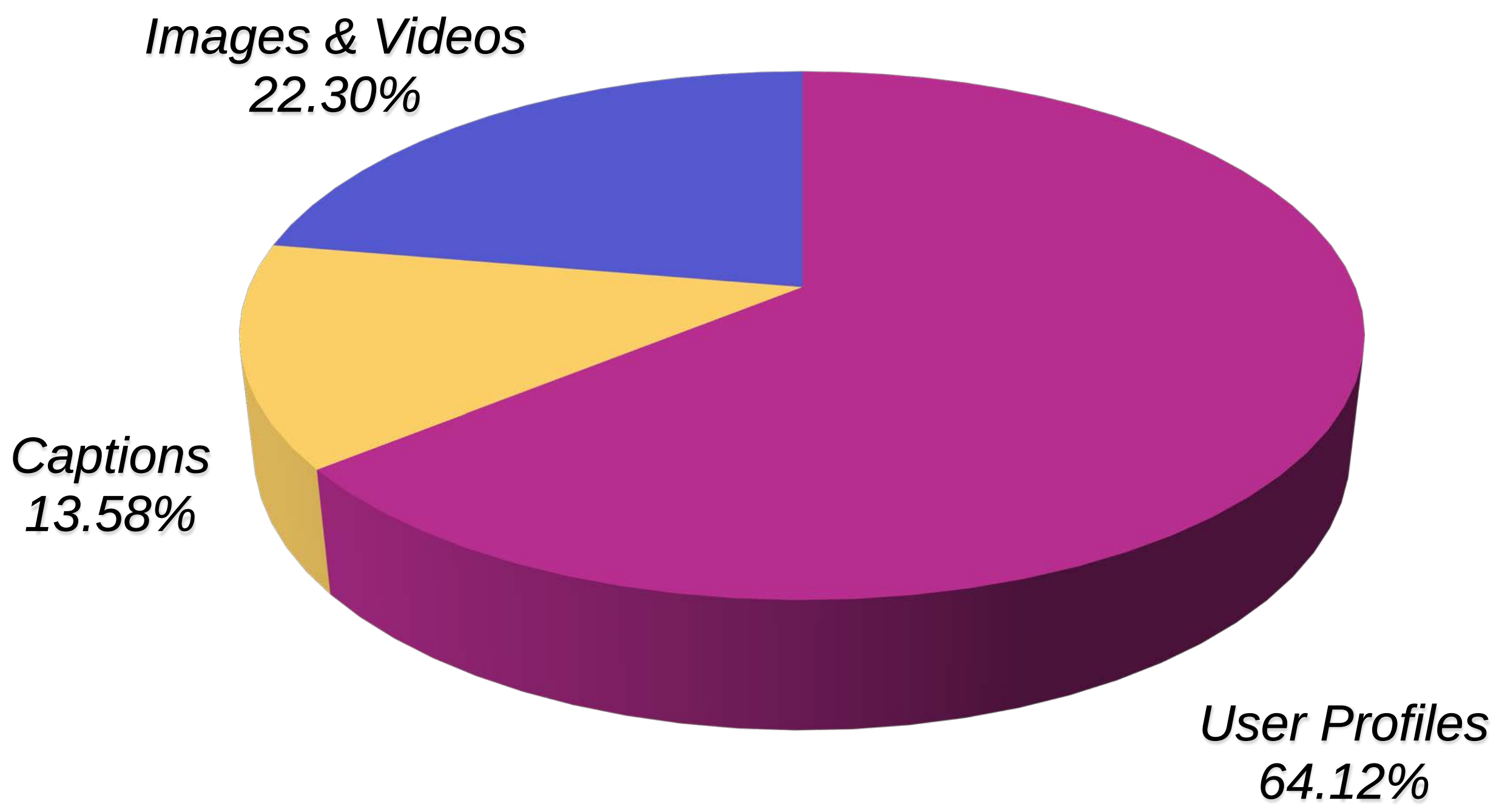
The units of analysis used for this study were ten user profiles, out of the 31 randomly selected, that met the study's requirements. In order to ensure only active accounts were included in the study, the hashtag filter "*#trending*" and the subheading "*Most Recent*" were used to find profiles and subsequent posts from the same user-account. This also included the analysis of a total of 50 posts, five from each of the ten profiles, posted within the time frame of January 1st, 2017 to December 31st, 2017. Each profile and post was assessed based on user-created captions, and the content within the images and videos users shared.

In order to ensure greater accuracy of capturing what was divulged by users, only manifest content was used in this study. This was due to the nature of content sharing, where posts are not always of, or created by, the profile owner. Information that included personality features, opinions, likes and dislikes, etc. was not included, as it is more subjective and not a major feature in identifying a person online or offline.

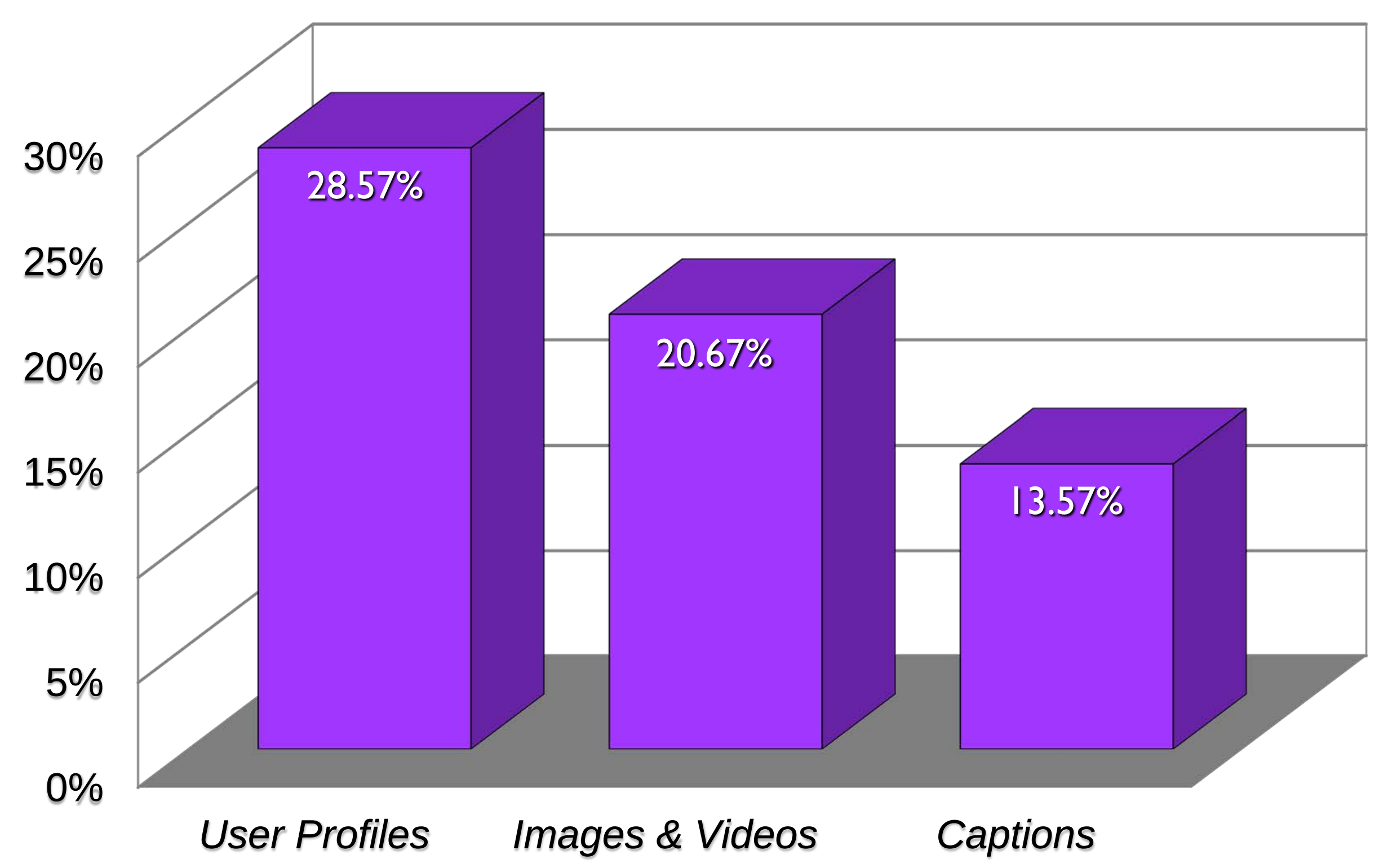
Results

Instances of personal information were open-coded by the three methods of sharing: (1) user profile content, (2) captions, and (3) image and video content. Subsequent coding identified 15 distinct themes for each method of sharing.

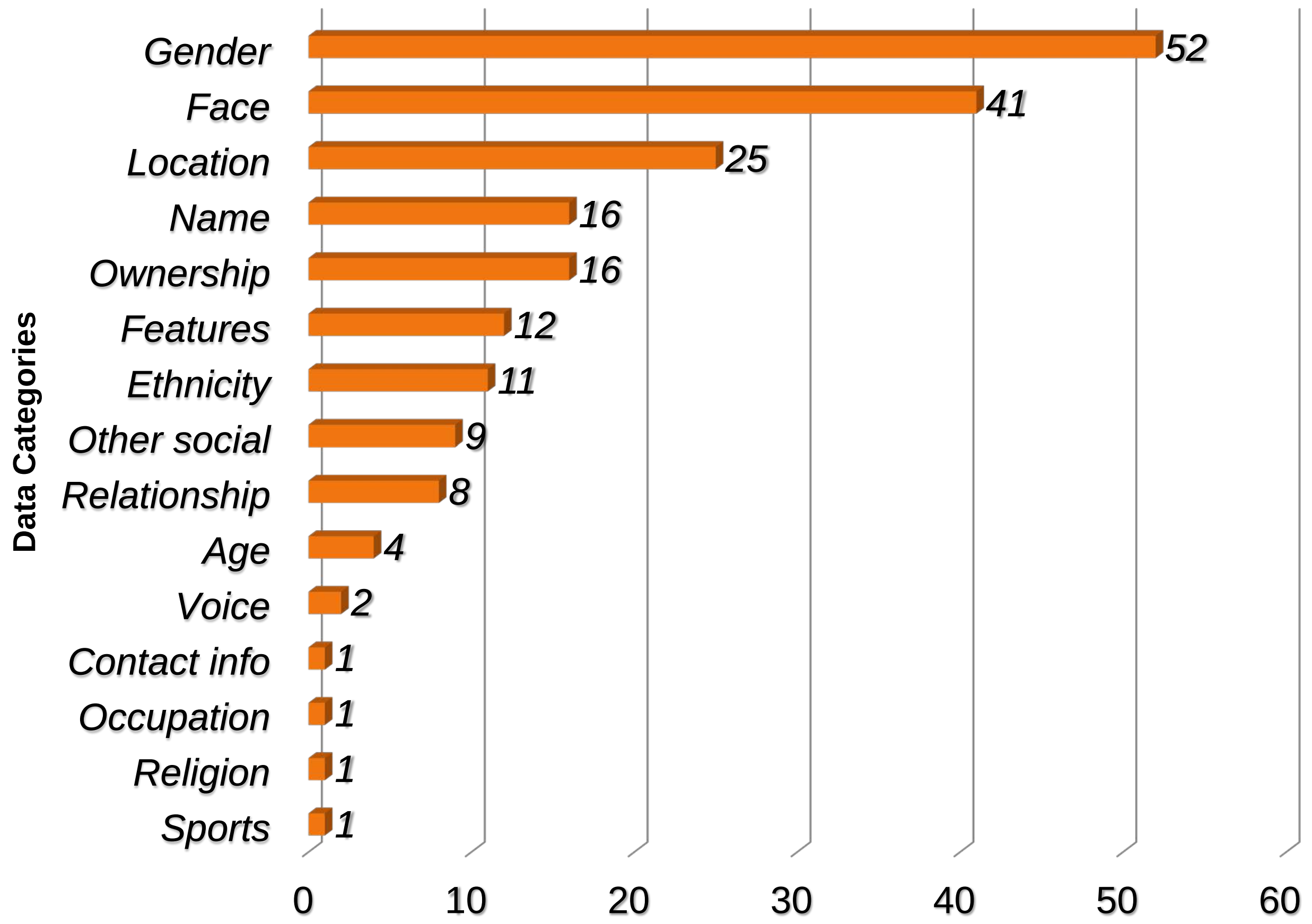
Where Information Was Shared



Range of Information Shared



Total Instances of Shared Information



Conclusion

Zemmels and Khey (2015) recognize four digital media traits that create security risks: persistence, searchability, replicability, and scalability. When an individual posts online, they leave a data-trace that is searchable, recordable, copyable, and shareable. Due to the ease of reproducing information online anonymously, users are not capable of overseeing or fully knowing their entire audience (Hogan, 2010; Livingston, 2004).

Users recognize the risks, yet continue to share personal information online as a vital exchange for personalized services such as online banking and shopping (Buchanan, et al., 2007; O'Neil, 2001). In this way, personal information becomes a currency to use "free" Internet services, where third parties can monitor and sell this information to other businesses (O'Neil, 2001). However, while there is a known possibility of third-party services retaining and selling personal information, there are more insidious threats and risks.

Identity theft can occur online and offline, by using another individual's personal information to impersonate and exploit them (Hille et al., 2015). Using a *femtocell* – a device that intervenes and records phone conversations, text messages, and images sent through cellphones – is one of the many ways that this information may be obtained (Zemmels & Khey, 2015).

Along with the possibility of financial losses from identity theft, reputational damages may also occur, such as an individual's name being associated with illegal or embarrassing purchases (Hille et al., 2015). While the effects of a damaged reputation are less studied, the impact is just as harmful to quality of life (Hille et al., 2015). Thus, the ways in which information is considered private and used need to be explored further in order to remain relevant for Internet security purposes (Lange, 2008).

References

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*, 157–165.

Hille, P., Walsh, G. & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19.

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society, 30*(6), 377-386.

Instagram. 2018. Instagram help. Retrieved from http://help.instagram.com/

Instagram Image Source: https://app.clicdata.com/help/docs/connectioninstagram

Lange, P. (2008). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication, 13*, 361-380.

Livingston, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review, 7*, 3-14.

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17-31.

Zemmels, D., & Khey, D. (2015). Sharing of digital visual media: Privacy concerns and trust among young people. *American Journal Of Criminal Justice, 40*(2), 285-302.

Acknowledgement

The mentorship of Dr. Diane Symbaluk in Sociology 315 (Winter 2018).